Health Information Technology Policy Committee
Summary of the September 18, 2009 Meeting

KEY TOPICS

1. Call to Order

Judy Sparrow, Office of the National Coordinator (ONC), welcomed Committee members to the fifth meeting of the HIT Policy Committee. She reminded the group that this is a Federal Advisory Committee meeting and that it would be conducted publicly.

2. Opening Remarks

David Blumenthal, National Coordinator for Health Information Technology, welcomed the group and emphasized the Committee's focus on discussing issues relating to the privacy and security of personal health information that is stored and transmitted electronically in a health information system powered by electronic technology. He explained that the primary focus of this meeting would be on privacy-related issues. He thanked the members of a task force that represented the HIT Policy Committee in developing the agenda and related materials for this meeting—members of the task force represented both the HIT Policy and HIT Standards Committees. In his role as the National Coordinator, he will be carefully considering today's testimony, as well as the recommendations that were recently made by the HIT Standards Committee regarding privacy and security issues.

David Blumenthal suggested that during its next meeting, the HIT Policy Committee discuss the next set of issues within its mandate, for example, the Nationwide Health Information Network (NHIN), and how that should be organized and governed going forward. The ONC has been tasked with developing governing mechanisms for the NHIN, and there will soon be rulemaking on that topic. David Blumenthal will be working to coordinate agendas with the National Committee on Vital and Health Statistics (NCVHS), which has conducted work on privacy and security issues and will be a resource for the federal government on topics related to data use and exchange and privacy.

3. Review of the Agenda

Committee Co-Chair Paul Tang reviewed the meeting's agenda, noting that this meeting represents an informational hearing, and that there may be other ways in which the Committee obtains input in the future.

4. Review of Privacy and Security Policy Issues

Jodi Daniel, ONC, offered some background information on privacy and security issues. She reviewed the policies that are in place today, since the American Recovery and Reinvestment Act (ARRA) builds on this foundation. The most prominent of these are federal privacy laws and Health Insurance Portability and Accountability Act (HIPAA) privacy and security rules, but there are others as well, including rules regarding substance abuse treatment information.

HIPAA sets a floor for protection, and allows state laws to exceed those protections. This creates some challenges to those trying to comply.

Last December, a framework with high-level principles for privacy and security was created, and those principles were used as a basis for setting up the panels for this meeting. Jodi Daniel noted that 42 states and territories have examined their policies and considered how those state policies affect interstate exchange. With regard to ARRA, some of the most notable changes are those dealing with business associates. For example, if an entity makes it so that information is not usable to someone who obtains unauthorized access to it, there is no need to provide notification that there has been a breach. This pushes groups to use heightened security measures for their information so that they do not have to initiate a breach notification. This is a safe harbor measure; it is not mandated, but encouraged.

Jodi Daniel noted that there are many changes because of ARRA; she reviewed the changes and additions to the rules and their enforcement. She pointed to available reports, studies, and education requirements regarding HIPAA and ARRA privacy and security.

Jodi Daniel also discussed when the regulations were implemented and enforced, and presented the "ARRA 8" that apply to privacy and security. She also described the role of standards, both in terms of technology and best practices. She reviewed the Privacy and Security Workgroup's recommendations, and pointed to reports and white papers already created and planned. The ONC can generate more white papers, as it wants to provide support to and receive guidance from the Committee.

5. Patient Choice, Control, and Segmentation of Health Information

Deborah Peel, Patients Privacy Rights and the Bipartisan Coalition on Patient Privacy

Deborah Peel said that her organizations believe that "the cart is in front of the horse" concerning these issues. Standards and plans have already been formulated, but privacy issues are actually foundational and belong at the beginning of the process. Ensuring control over data is the only way to create a trusted health IT system, a system in which people trust their doctor not to share data without their permission. Any discussion of patient choice, control, and segmentation of health information should start with the following facts:

- Americans care deeply about the privacy and control of their information. A majority of Americans think that they should own their own data.

- There is universal agreement that patients should have a say in how this information is shared and used.

- A majority believes, as a broad principle, that it is no one's business to know about their personal health care information.

- Participants overwhelmingly want to communicate with their providers about how their data is handled and shared, and for what uses. They automatically think they have a right to correct misinformation.

A 2005 California health care survey showed that Americans are already taking action to hide or omit data from the health care system. Additionally, the Institute of Medicine found that only 1 percent of Americans would ever agree for researchers to have unfettered access to their information. Approximately 80 percent oppose having their information used, even if the information is de-identified, without their knowledge. However, 87% of Americans support research—the point is, they want to be asked.

The right to privacy and control is the national consensus, she said. The thought that there is not a consensus around the question of who should control health care information is not true; there is a consensus. The public does not support having general, one-size-fits-all rules in terms of privacy policy. The good news is that technologies exist now to allow a more personalized approach. Consumer control over their own data is the cheapest, easiest, and most efficient way to get data to flow. Deborah Peel asked that people keep this in mind as the conversation moves forward into complex ways of sharing information. There is no need for a complex legal agreement, she said, just ask the patient.

Data mining, secondary, and tertiary information use is a multi-billion dollar industry. This industry is not going to reform unless they are given a clear mandate. Deborah Peel suggested three ideas that would make the system work: (1) no protected health information should be exchanged without informed consent; (2) patients should have a place for electronic data to be sent at no charge; and (3) patients must be able to selectively segment sensitive information; segmentation and audit trails will be necessary to demonstrate to the patient that that their information has been handled in the way that they want.

Deven McGraw, Center for Democracy and Technology

Deven McGraw agreed that consumers want their privacy. They also want their data to be accessible for the best health care for themselves, and they want to be able to control it. She said this is a really intuitive and appealing solution, and it does not surprise her that people in focus groups and surveys would indicate that they want control of their data. However, consent does not work seamlessly for creating privacy. Over-reliance on consent actually provides very weak privacy protection. The limits of consent were illustrated in a recent news item—health and life insurers obtained personally identified information from data miners, and this revelation caused much consternation, but in fact that data was in the hands of the data miners because the patients consented to the use of their data.

Health care does not present good opportunities for people to say "no," which is why consent does not work well to protect privacy. Consent relieves the data holders from the responsibility of protecting data and can lead to less incentive to design systems that are secure and protect against risk. The role of privacy should not fall to the consumer, who has to sign a form. Deven McGraw was told by a compliance lawyer that the easiest way to get compliance is to obtain patient consent. The language used on consent forms is often very broad and/or very

complicated, naming things like "research" and "health care quality improvement." Consumers may not be able to discern what these terms actually entail.

That does not mean there is no role for patient consent, which must be layered on top of a comprehensive set of rules around how organizations use information. For health information exchanges (HIEs), use and exchange of data is for more than treatment. But for personal health records (PHRs), this is a record that is a copy of the medical record for the patient to use. A strong case can be made that a PHR belongs to the patient, but this is not currently the case, per federal law. Deven McGraw noted that the e-commerce marketplace provides a good illustration of why a comprehensive framework establishes trust better than simply consent. These systems work because there are rules that require security to be in place and hold the individual harmless if there are errors.

Marc Overhage, Regenstrief Institute

Marc Overhage offered a case study of how an HIE has approached patient engagement and individual choice. He then explained that participating clinicians and providers subscribe to a series of principles. Participating providers have signed an agreement requiring them to follow privacy and security safeguards within their organizations. Providers inform patients through HIPAA privacy practices—this is when patients can discuss with their providers the uses of their data. He gave the following example: in order to create a virtual patient record in the emergency room, the system must receive notice that the provider is authorized by the network, and the physical computer must be located on the site where it is claiming to be. Also, because emergency care generally does not last for longer than 24 hours, the information is only available for up to a 24-hour period. Also, any time a virtual patient record is created, a permanent audit trail is created. That information is available to the patient through their provider. Participating providers decide together with their patient what information will be made available.

Susanna Fox, Pugh Internet and American Life Project

Susanna Fox noted that it is important to focus on people's actual behavior, and not just the hypothetical, not just their attitudes. People will say one thing, and do another. During her comments, she focused on how people use the Internet to gather information. Patients frequently route around advice from their doctor to not use the Internet as a source of information. Because they cannot get what they want from current health care system, patients are creating their own ways to gather and share health care information.

Susanna Fox emphasized that privacy and security are absolutely foundational requirements, but they are not the end goal—health is the end goal. The latest data from her group indicates that the American people have a different idea about access to information in that they feel that they should have access to "industrial strength" information, not "consumer strength" information. This is true in health care, and in other arenas as well. In political campaigns, more people are watching the actual speeches and reading the actual campaign documents, not just watching TV coverage. Likewise, people are actually reading medical journal articles, not predigested media analysis. Susanna Fox shared some comments that she received on her e-patients blog after she posted this testimony:

- One reader said they wanted innovation at a rate that approaches the rate of improvements of cell phones and iPods. He echoed what Deborah Peel said: "You bet I ought to be able to get my hands on all the data, proofread all of it for accuracy, take it wherever I want."

- Another noted that consumers with diverse perspectives, circumstances, and experiences must be included in the design of culturally sensitive tools. This reader asked that mobile technology be included, because "that is the future."

Patient-generated data represents a new pool of research data that has the capacity to improve outcomes data. Technologically speaking, where the industry now is the Web. Where it is going to be is in the realm of mobile and patient-generated data. Many people are working outside the system right now. She urged that they should bring these people in and make them part of the solution.

Discussion

Paul Egerman invited questions—the ensuing discussion included the following points:

- Marc Overhage discussed accounting of disclosures. He said their general approach is that this is an issue between the patient and their provider. They are the custodians of the data. His organization, as the HIE, facilitates disclosure but is not involved in it, because they have no relationship with the patient, nor can it authenticate the disclosure. They simply facilitate access to that information, while the provider and patient decide how the information will be made available.

- With respect to health care operations activities, Deven McGraw said that from a consumer advocates perspective, it is perplexing. Some consent forms are broadly worded to provide doctors with a fair amount of discretion. There is a need to be able to use some patient data in order to function. On the other hand, big categories that say "administrative activities" and the like, are troubling. She would much rather offer incentives for using data responsibly.

- Deborah Peel agreed that "health care operations" is a troubling category—it is the main category of open use for providers, including the sale of data. She believes that if the health care entity can explain in a clear, simple way how they want to use the data, people will agree to its use. She also explained that there has never been any research demonstrating that that consent does not work. Instances of consent not working are examples of coerced consent, or blanket consent.

- With regard to e-commerce, Deborah Peel noted that people trust that banks handle their money the way they want them to, but they do not have privacy over financial details.

- Deborah Peel also commented that any discussion about consent, has to focus on "meaningful consent." Very detailed consents have been working effectively for the exchange of sensitive data.

- In addition, Deborah Peel noted that the National Data Infrastructure Improvement Consortium (NDIIC) is a national open source organization that has developed granular health exchange that works well. Those standards are very easily translatable by HL-7.

- Frank Nemec, a gastroenterologist, noted that in his practice they have been careful about patient confidentiality. In the 2 years since the practice has adopted use of electronic records, it has become easier to comply with HIPAA. However, insurance companies have control over the medical information—people that his patients do not know and have no control over. Patients lost that control many years ago, he said.

- Gayle Harrell noted dealing with the privacy and security of electronic health records is a foundational question that requires conversation that needs to be very public. There is a great deal of concern on the business associate side of things; information is being sold and used, and this is the number one concern she hears from consumers.

- Deven McGraw reported that there are some new provisions that strengthen the enforcement of HIPAA rules on business associates. However, there is another problem in terms of how data travels down the chain, and this is not addressed in the ARRA legislation. Some of this is anecdotal, she noted, explaining that business associates are getting data from one covered entity, and then acting like the data belongs to them. This could be fixed by creating stronger rules about what the business entity can do with the information. They must perform the function that they were asked to perform, and that is the end of its use. The law is there, but it is not clear enough and has not been appropriately enforced.

- The question was asked, at what point does consent become so cumbersome that it hinders cancer research? Deborah Peel acknowledged that there is a big fear that consent will interfere with research. However, it easy and inexpensive to contact people now, thanks to advances in technology.

- Judith Faulkner noted that information is threaded throughout a patient record, so it is difficult to hide a condition because there is evidence of it in the notes, the imaging, the labs, the results, the orders, etc. It can be very misleading and unfair if patients think that technology can hide all threaded information. It also compromises the quality of care. Instead of focusing on penalizing for information that gets transferred, should the issue be about penalizing if the information is inappropriately used?

- Deborah Peel noted that privacy is not in the patient's control unless they are able to control that information, wherever it is. The protections have to follow the information.

- Deven McGraw agreed, commenting that on social networking sites, consumers play a strong role in controlling their data. If they want to put their data on some web site, that

is acceptable, but even if they consent, there should be some rules that govern how organizations collect and use/misuse data. There is currently no consumer privacy law at the federal level to protect people who use those sites; this is a gap that needs to be filled.

- It was noted that when people are facing death, sometimes they are willing to give up their information. Is this coerced or is it practical? In some cases, there is no privacy. This is an opportunity to learn from what Facebook learned, and what Twitter is working out this week, regarding who has control over what one does and says online. People are getting benefits from doing research and sharing data online. One person commented that health care is way behind this curve in this regard.

- One Committee member noted that informed consent is confounded by the fact that as the complexity of consent increases, understanding goes down. This can be seen with research consent. Consent language phrased at a ninth-grade reading level, with cultural sensitivity, gets backed with 12 pages of federally mandated language that everyone knows people do not understand.

- Deborah Peel suggested that a panel be convened with experts on consent to guide the Committee on how consent can be interactive and intuitive.

6. Use, Disclosure, Secondary Uses, Data Stewardship

Eileen Twiggs, Planned Parenthood Federation of America

Eileen Twiggs said that for most of their patients, Planned Parenthood is their sole provider. Their patients deserve the benefits that come with HIT, and they are moving forward with an understanding that sensitive information is going to be handled, and they expect that all risks will be appropriately addressed. There are individual, organizational, and societal reasons for going to Planned Parenthood, she said. Many come because they do not want their family or employer to know about this care.

Consider a 30-year-old woman in an abused marriage. Her previous treatment at Planned Parenthood is not something she wants her husband to know about. What happens if her husband takes her to the emergency room, and the clinician there is an anti-choice activist? The release of private information could lead to acts of discrimination or violence. She believes that there are five critical principles, as follows:

- We must protect the original understanding developed between the patient and provider. We have to honor the contract. Decision-making authority must remain at the original point of care.

- Participants in the exchange should access only the areas of data they need to give care.

- Policy must define that once information has been declared confidential, it will always remain confidential. Clear standards must be developed for all participants. Patients will expect that their information will remain confidential wherever it goes.

- Inappropriate access must be denied within and outside the continuum of care. Those without a genuine need for access must remain at bay.

- Privacy and security breaches must be proactively sought out and penalized. There should be heightened criminal liability and professional sanctions.

John Houston, University of Pittsburgh Medical Center

John Houston pointed to two NCVHS reports: one on privacy and confidentiality specifically related to NHIN and sensitive information, and one on data stewardship. He said he is sensitive to privacy and security issues, and also pragmatic about the delivery of health care. There must be a balance. The problem he sees with privacy is that it is a societal value, and that each person in good faith has a different opinion about what privacy is and what it means. Regarding security, whatever is put into place must be flexible because new technologies evolve and new threats emerge daily.

It is vital to have some type of oversight process at the macro level. There needs to be a central organization that coordinates privacy and security. This organization would be responsible for credentialing participating providers and allowing patients to see where their information has been disclosed. One of the strongest vehicles for ensuring that people do the right thing is to show patients where their information has gone. ARRA provides for that at the covered entity level, but once information starts to pass across the United States, it is going to become much more important, and more difficult, for patients to see where that information has gone. This organization needs to be able to investigate inappropriate disclosures. Also, patients must be able to limit information sharing.

James Golden, Minnesota Department of Health

Jim Golden commented that public health agencies provide the backbone for the public health infrastructure, but other entities also are important to public health (e.g., hospitals, universities, clinics, etc.). Public health has a long history of protecting health care information, because this area has a long history of collecting such information. This information is necessary to carry out mandated activities, and health information exchange has tremendous potential to further the work of public health.

Detailed frameworks for public health privacy have been extensively discussed and debated in state legislatures, and reflect a balance of public and private concerns. States need to continue to play a lead role in public health policy, as they are better able to reflect the values and desires of stakeholders involved. Currently these frameworks are not uniform, and they are not simple.

He said it is important to keep four things in mind:

- Public health plays a critical role in protecting the community.

- It requires individually identified data in order to protect public health and the population.

- The privacy and security frameworks for public health reflect stakeholder interests and the perceptions about the public health threat, and the need to balance public health goals with other important public policy goals.
- There are tremendous differences between local and state policies.

There are, however, some characteristics that apply to various public health frameworks. These include: (1) defining the ability of the individuals to participate in decisions to collect, use, or disclose identifiable data; (2) the ability of an individual to know when and to whom their information has been disclosed; (3) the ability of an individual to access and amend their information; (4) the ability to challenge compliance with legal and privacy frameworks; (5) the need to maintain role-based access to data; and (6) the need potentially to have time-limited access to data. Including population health and public health in the framework is an important use of HIT, and should be a part of the initial definition of meaningful use.

Discussion

Deven McGraw opened the floor for questions; the following points were made during the discussion:

- Jim Golden noted that if a patient has come to an emergency room unconscious, the physician needs to have as complete a medical picture as possible, including psychiatric treatment and associated medications. It is very difficult to understand exactly what information is necessary at a given time to provide treatment. He believes it is necessary to err on the side of more information, and more accountability, in order to make sure the right care is provided.

- Gayle Harrell asked for opinions on notification of patients when information is accessed, as a mechanism of putting controls in the system to empower the patient (e.g., up-front notification that a patient's information is to be passed to another entity). Eileen Twigg said that patients have a right to know when their information is being used and for what purpose. The concern lies in getting the balance of that information so that it is meaningful. For example, if a patient has the expectation that their information is going to be shared with their insurance company in order to get their bill paid, then they may not want to be given notice of that. However, when information is released for purposes that a patient is not expecting, then she thinks that would be an appropriate circumstance. She acknowledged that there are no simple solutions.

- Paul Tang noted that the Committee now has to start moving toward solutions to these issues, because data is going to be exchanged. This exchange can be handled in at least three ways: (1) put the burden on the patient; (2) trust but verify, putting burden on the provider; and/or (3) legislation.

- One commented that it is very difficult to get meaningful consent, and regulation is not an attractive option. It was suggested that the second option presented by Paul Tang—trust but verify—may be the best option. Between internally reviewing access as well as

providing transparency to the patient, those two things would cause the system to achieve some reasonable balance. There will still be some regulation needed, as well as some level of consent, especially for sensitive information.

- Another participant characterized this as a "false choice." In the case of infectious diseases, consumers understand that they might contract a disease through no fault of their own. They understand that their data needs to be shared. This is in contrast to chronic diseases, which are often thought of more as lifestyle choice consequences. The system has to be sophisticated enough to provide for options.

- Eileen Twigg noted that the exchange entity can play a role. Although she does not think they should have any part in deciding when or how information is released, it does have the ability to monitor and enforce exchanges, so it can understand how the community as a whole is acting.

- The following construct was also suggested: (1) classify the data to its degree of sensitivity, (2) classify users, and (3) manage the relationship between them.

- With regard to transferring information stewardship to patients as they turn 18, a Committee member asked for the panel to consider the ethical considerations. It was pointed out that another big issue will center on parents who have been tested for genetic conditions that their children want to know about.

- It was noted that, with respect to public health, things changed when bioterrorism and chronic diseases were put into the same category. There is a real difference between people being exposed to infectious disease on the subway, and chronic disease. Part of the policy component of public health is that it needs to inform the public about the issues and costs—that allows for targeting resources and interventions at a public health level.

- With respect to macro-level oversight of privacy/security, Jim Golden was asked whether he believes such governance practices are best made at the lowest possible level—that is, the provider organization. He was also asked about the role of the macro-level oversight body. Jim Golden replied that no one knows how widely information is going to be shared. It likely will be something out of the context of provider care, though. There needs to be ways that data can be aggregated, as transmissions go beyond a region. Provider credentialing is also critical, because some people are still not covered by HIPAA. Also, he said that he does not know if the Office of Civil Rights has a role regionally, but he believes there needs to be national standards and the opportunity to ensure that these are consistent across the country.

7. Models for Data Storage and Exchange, Aggregate Data, and De-Identification/Re-identification

Claudia Williams, Markle Foundation

Claudia Williams focused on three points: (1) we must adopt a framework-based approach; (2) policy must guide technology, and not vice versa; and (3) we must stimulate innovative models for both protecting and sharing information. These principles require that limits be set on data collection, that patients have reasonable controls over their information, and that safeguards are adopted. This framework has been translated into very specific health care sectors.
When data are needed, the purpose must be specified, and only the data needed to accomplish that specific task will be shared. Audit logs must be created, and information must stay as close as possible to its source. In contrast, technologically driven solutions often come to policy in an after-the-fact manner.

Claudia Williams presented examples of how these privacy principles can be the starting place for operational decisions about how information is shared across the health care system. These principles should guide and shape the clear policies and technology choices, including how information is discovered, exchanged, analyzed, and stored. In health information exchanges, the architecture can be such that the data remains locally controlled, which means data stewardship and control remains in the hands of those closest to the source.

Philip Marshall, WebMD

The PHR services provided by WebMD are provided in conjunction with employer agreements. WebMD is a HIPAA-covered business entity. Its purpose is to share data to support better health care decisions. Philip Marshall indicated that WebMD does not share health information with employers, though consumers can choose to do that.

There are some specific barriers to consumer-centric data exchange and access. For example, consumers cannot get their lab results directly from the lab; the results must be released by the ordering care provider. It is time to look at those legal barriers again and reconsider. Philip Marshall stressed the importance of not just technical interoperability, but also semantic interoperability.

WebMD supports the notion of certification of PHRs, through the Certification Commission for Health Information Technology (CCHIT) or other organizations.

Kenneth Buetow, National Cancer Institute

Kenneth Buetow explained that the National Cancer Institute (NCI) conducts research within the National Institutes of Health (NIH). The NIH and NCI sit at the interface with care, and he thinks their work will be transformed with HIT. They have a broad depth of experience in managing information regarding clinical trials. They work with large, time-monitored cohorts, and maintain aggregated, de-identified registries. This includes managing exchanges between multiple communities. He qualified that he was not speaking for the NIH or NCI, and pointed out that in his submitted testimony he described the information flows with identified, de-identified, and aggregate information. One size absolutely does not "fit all." Information architectures are needed that recognize that data has to live in all these forms, and be transformed between these different pieces.

Kenneth Buetow noted that definitions are important, and structure is key. Discipline in data collection is important (e.g., who has access to the data and under what circumstances?). There must be an architectural framework around this—not a specific, proscribed technical solution to a problem, but a semantically interoperable framework that allows for a description of the facts about the data. In this way, it is possible to manage who can have access to what. Also, it is critical to manage consent, and to recognize the importance of consent where it is manageable. The burden of consent can be heavy in different areas in various circumstances. Emerging architecture/technology is beneficial because it will allow us to tag consent in either blanket or granular fashion.

Attribute-based access layered on content-based security is a real possibility and one that the NCI has deployed in its network. The Institute can track who can do what to what, and in what context. It is important not to create a regulatory framework that specifies every instance of what cannot be done with the data. Instead, there should be consequences for its misuse. Also, policy makers should do no harm. Research is already a very bureaucratic system; as new rules are passed, they must not create a viral, unintended reach-through that cripples existing processes.

Discussion
In discussion, the following points were made:

- Claudia Williams noted that the demonstration of meaningful use could be accomplished simply through regular use of the system. This would lessen the burden on the provider, and would allow better achievement of quality control and audit.

- It was noted that the availability and use of aggregated data is going to be essential. The engine that drives this underlying decision support is aggregated data. Caution must be taken when the word "aggregated" is used; it does not necessarily mean that it is completely de-identified information. One of the ways this is dealt with in the clinical research arena is to be completely honest that participants are not always going to be completely anonymous.

- In response to the question of how, as a policy matter, this Committee should think about architecture, Claudia Williams said that it would be helpful for them to say, "here are the principles and guidelines that must be considered when creating architecture." Federal dollars should be used to cultivate models, rather than assuming that there is only one architecture that must be central. Many HIE efforts today are using a federated model; there is a lot of experience about how that works and also many questions that need to be answered. She suggested that the committee could play a huge role by saying to states, "here are five examples that are working today. You all should be talking."

8. Transparency, Audit, Accountability

Robert Gellman, Consultant

Robert Gellman explained that for any fully computerized system, it is essential that there be an accounting of all disclosures and all uses. That capability already exists; the celebrity snooping example is a good one to illustrate this point. Such accounting needs to be done consistently and thoroughly. Without accounting, medical theft identify will become a serious issue. Patients should have online access to this accounting, and be able to control the extent to which they get notified when people see their records.

Also, he noted that if a record exists (whether its existence is required or not by law) the patient should have a right to see it. Any new requirements for accounting should be prospective only. Nobody should be asked to account for disclosure of oral or paper records; retrofitting would be extremely expensive.

Unless a record is kept of those disclosures when a patient says it is acceptable to share information, it will not be possible to go back to an entity and instruct them to stop. A patient could spend years going from one business associate to another just to find out if they have his or her records, let alone whether they have disclosed them. A major hospital could have hundreds of business associates.

The ARRA legislation included a provision, which Robert Gellman called "pass the accounting buck." It indicates that a covered entity does not have to keep track of disclosures or provide an accounting of disclosures by business associates. Instead, the covered entity can just give a patient a list of business associates and the patient can then go pursue all of the business associates to find out what they did with their information. Current HIPAA laws ask the provider to give a good faith notice that patients received privacy notices. He characterized this as just a paperwork requirement and said it ought to be eliminated. Patients should have notices when they want them. When the patient has a concern, they will seek out a notice, read it, and pursue their rights.

Robin Omata, Kaiser Permanente

Robin Omata presented the following main points:

- Health care dollars must be directed to measures that help patients.
- Accounting and transparency are already largely accomplished through HIPAA.
- With respect to ARRA, she suggests that the disclosure accounting requirement as currently written does not add value relative to the cost of implementing the requirement as it is currently written.
- The meaningful use measure that uses a confirmed HIPAA privacy and security violation as a basis for measuring privacy and security protections of the EHR should be revised or eliminated.

Kaiser has an online health care portal, which patients can use to refill prescriptions, communicate with doctors and clinicians, see lab tests online, and make appointment requests.

She said they are already connected and take very seriously the capabilities and functionalities of the system, as well as privacy and security. This is not a single entity or a single system, it is a "web" of systems.

Robin Omata commented that with regard to the disclosure accounting requirement, without further clarification as it is written in the law, it is troublesome, expensive, and does not help the patient. She suggested that further refinements be made to the provisions regarding privacy and security. Specifically, the measure uses a confirmed HIPAA violation as a measurement. This bears no direct relationship to privacy and security in the EHR. They should instead consider applicable security standards within the EHR itself and with regard to exchanges and interoperability.

Discussion

- Bob Gellman suggested that the reason organizations such as Kaiser do not receive more requests for audit trails is that the accounting records that are required by HIPAA today are useless. For most people, there is not much in the records worth asking for. On the other hand, before there were EHRs, there were very few requests for them. Once it was easy and the records were useable, people really wanted them. The same thing would be true, he said, with actual, useful auditing.

- Robin Omata suggested that a fact-based decision making process is missing. A number of issues or levels of consumer demand are being asserted that she has not seen documented in national or regional surveys. That said, she did not dismiss the need for accounting. There is, however, the question of a cost-benefit equation. For that there are other competing requests, which are documented, to improve and upgrade reporting systems. She did not dismiss the seriousness of providing for a patient's records, but she emphasized that they must not overburden the system with something that is relevant to only a very small part of their membership.

- Bob Gellman noted that the records are important whether they are used by patients or not. There are many reasons to do accounting for disclosures.

- Gayle Harrell commented that cost versus privacy accountability is at the heart of this issue. The public may not be requesting their records right now, but as the country moves into the level of EHRs that this Committee hopes will exist, this will become extremely important. People want to know that their information is accountable. It may be expensive, but privacy and security must nevertheless be the foundation. Without having audit trails and documentation, there is no accountability. In order to know what happens at the end of the day and who is responsible, there must be enforcement—but documentation is needed in order to have enforcement.

- Robin Omata noted that Kaiser's records are already segmented and wondered which of the 80 million or so transactions might be the most sensitive.

- Bob Gellman insisted that the accounting records already exist. It's a matter of translating them into a more useful format for patients that needs to be addressed. Congress has already specifically asked for more accounting.

- It was suggested that a white paper may be needed to illustrate specifics of ARRA around disclosure. The majority of systems providers probably do not now comply.

- Jodi Daniel asked Robin Omata if there is one area of this process that is most expensive. Robin Omata indicated that it would be in the programming to identify, trace, and bundle all the sources of information, and then to assign a new English language explanation as to the meaning of each audit trail item. She suggested that the granularity of the information available in the audit trail may not give a level of satisfaction to the patient. She said Kaiser is asking for clarification so that they can find out what would be useful to the patient. The biggest expense would be in the actual code development, and also the front end and back end research about what would be useful.

9. **Comments on Constructing Provably Appropriate Technology**

LaTanya Sweeney, Carnegie Mellon University

LaTanya Sweeney noted that she has spent a great deal of time exposing fallacies in privacy mechanisms, and revealing what does not work. In her prepared statement, she offered a list of those related only to HIPAA, but they extend across many other domains as well. In her view, technology design radically changes all of the discussions today. If five different designs were put on the table and each of today's speakers were asked to come back again, then they could describe why they like this part of the design, and why they hate this other one. The Centers for Medicare and Medicaid Services (CMS) has published an RFI asking for input on how best to rebuild the system, but industry is likely going to come back with a retooling of what they already have on the shelf.

A group of academics have decided that they can help to bring industry and stakeholders together to make sure that the technology and the decisions made are well informed. They have committed themselves to this and have a name: the Advanced HIT Project (advancedhit.org). Everyone is very enthusiastic, including industry partners. The outcome will be white papers, and they will be open for public comment. Carnegie Mellon, Harvard, and MIT are the three primary partners, but they will be reaching out to other experts.

Discussion

The discussion that followed including the following highlights:

- LaTanya Sweeney noted that the best solutions are in the technology. For example, if Twitter is a problem, the best way to handle it is to change Twitter, not to create an add-on. Even the issue of the audit trail will change with technology.

- Christine Bechtel asked LaTanya Sweeney to discuss the issue of data use, focusing on patient concerns about downstream uses. How would architectural design impact the use of data down the line? LaTanya Sweeney said that the meaningful use matrix is a great guideline, but there are facets of Meaningful Use that are not in the matrix—they come up in the conversations about meaningful use, but they are not actually listed in the matrix. She also commented that it is difficult to imagine any complete solution without a data infrastructure. Some of those uses might be ways to save money, like medical identity theft. Those are all policy decisions.

- Christine Bechtel suggested that this Committee must do some real work around identifying the beginning set of policies that would move this effort forward. Then, if it can put those up against a set of potential architectures, that would be beneficial. She encouraged the group to commit to crafting what that set of policies looks like, how it builds on the work of all the people they have heard from today.

- LaTanya Sweeney agreed, but noted that having a discussion on policy in abstraction is not going to serve them well. She is not suggesting they focus architecture and then policy, either; this is iterative design, they must bounce between the two.

- David Blumenthal indicated that the Committee needs to discuss next steps and digest what it heard today. The Committee must reconvene the task force that put this series together and have that group propose a set of activities for the HIT Policy Committee going forward. He suggested creating a menu of short, medium, and long-term activities.

10. Public Comment

Deborah Peel reiterated her group's offer to help bring the consumer perspective on privacy into this process.

Joy Pritts of Georgetown University noted that a lot of work on privacy and security has been done by other countries. The United States may or may not wish to copy their solutions, but white papers already exist. She suggested that Canada has a very thorough analysis of privacy and security, and they have almost an abundance of information, very useful and organized, about how to segregate information, including vendor conformance requirements, etc. All of this information is available for free online.